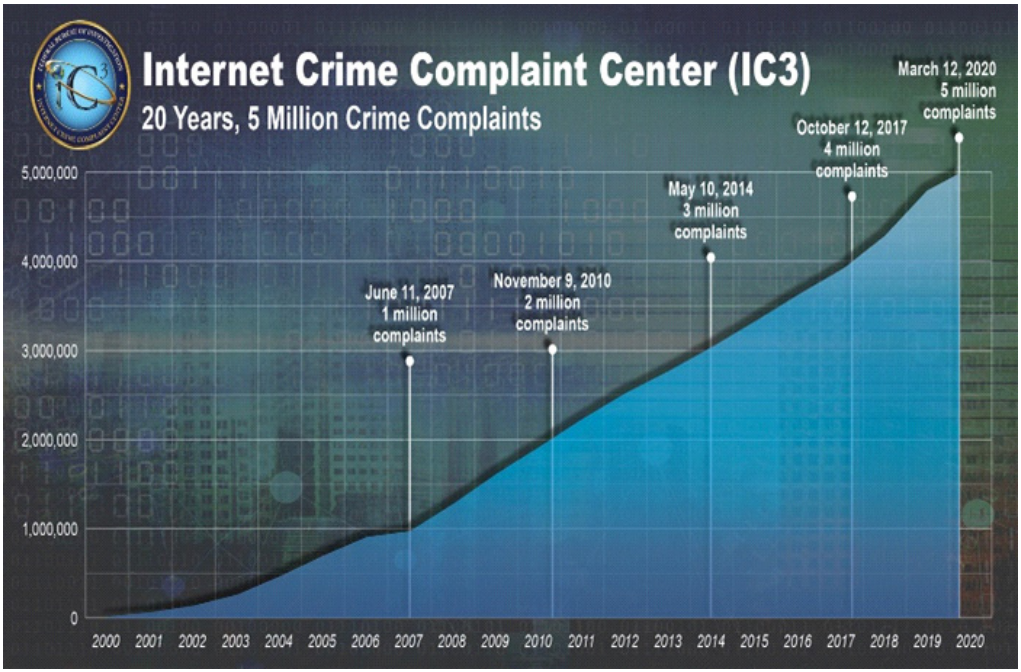
Technology: Opportunities and Challenges for Criminal Investigations

Michael Breslin

Robert G. Lowery, Jr.

2021



Internet Crime Complaint Center (IC3) trend chart

Technology: Opportunities and Challenges for Criminal Investigations

Technologies, both existing and emerging, have paid enormous dividends when it comes to protecting communities, identifying criminals, and solving crime. The Internet, social media, digital camera capabilities, license plate readers, and cellular and smart phones have been successful “game changers” when it comes to suppressing and controlling crime. The good news is that criminals can no longer rely on anonymity when performing nefarious acts — the likelihood they will be caught is higher today than ever before. According to the FBI Uniform Crime Reports (UCR) over the past several years, there has been a significant downward trend in “traditional street crime” — burglaries, robberies, larcenies, and even homicides.

The bad news is criminals have long been aware of the capabilities of technology — how it is used to commit crime and how law enforcement uses it to catch them. We now see evidence of countermeasures while committing street crimes, such as altering appearances, turning off smart phones or simply leaving these devices behind, the widespread use of “burner” phones, concealing license plates, the use of stolen cars, and others. Many have shifted their activities from traditional street crime to the Internet or cybercrime, where they face far less risk of detection, identification, arrest, and prosecution, not to mention that committing street crimes almost always comes with the risk of violence for themselves and their victims.

Police administrators often point out that improved policing methods, enhanced community relations efforts, and innovative tactics deserve much of the credit for reduced crime rates, but technology, with little doubt, plays a significant role in crime eradication. That is certainly good news, but it does beg the question, “While technology obviously has contributed tremendously to reduction in street crimes, have we actually stopped criminals from committing crimes?” The answer is both yes and no. Technologies have, with little doubt, discouraged street-level criminals from

committing their acts while others have transitioned to committing cyber or technology-facilitated crimes.

The improvements in traditional crime deterrence have no doubt reduced crime but have not necessarily stopped those from achieving their ill-intended goals. Criminals will eventually find ways to defeat or minimize the new and emerging capabilities. We must continually look to improve capabilities with new or improved innovations.

While traditional crime remains a priority for law enforcement, technology, the Internet, and social media have created a “new frontier” where criminals may now freely operate — albeit with a greater degree of sophistication and secrecy. Criminals find many benefits in the cyber world, including a broader scope and greater numbers of potential victims (their crimes can be committed on a transnational scale), the fact that cyber-currency is difficult to trace, encryption, the deep web, and the dark web that conceals their identities and activities. Law enforcement now faces a new breed of scofflaws. [1]

The Internet, social media, and technology have contributed greatly to making our world a much better place but, like anything else in our world today, there are those who use these innovations and contributions for illegal and illicit purposes. Hence, the challenge for law enforcement — we must be better prepared to adapt to this changing environment.

Awareness and recognition of cybercrime and trends, staying current with the latest countermeasures, continued advanced training, enhanced and increased analytic capabilities, and recruitment of personnel with the skill sets necessary to respond to these threats are some of the areas that require our full attention. Many agencies are simply not prepared, for a variety of reasons, especially in today’s environment of static or diminishing budgets and resources. Curbing crime over the long term will always be the biggest challenge as it means changing human behavior by reducing criminal motivation or influencing “what lies in the heart of human beings.” This will not be solved by the application of technologies or law enforcement acting alone. Those intent on committing crime will most likely continue to do so, regardless of how effectively they are discouraged or impeded.

The changing landscape of criminal investigations because of technology, coupled with the current high turnover (retention and recruitment) in law enforcement, compounds the issue. The length of time on the job for new detectives and homicide investigators of two to five years is not uncommon in many agencies today.

We are experiencing a transformation in how criminals are using technology to invent new crimes and are creating new ways to commit traditional crimes. Successful mitigation necessitates the actions and collaboration of law enforcement personnel across all branches and jurisdictions. Cooperation and information sharing between agencies is key to enforcement and keeping up to date with new and emerging trends.

While not an exhaustive list, the following are three general areas which currently affect law enforcement activity, investigations, and resources at all levels (federal, state, and local).

1. Prevention and suppression of crime — safety of communities
2. Criminal activity carried out on the Internet and social media
3. Criminal Investigations — data sources: victims, witnesses, suspects

Many communities are embracing and equipping themselves with the latest technological advancements to improve quality of life, monitor and manage traffic conditions, identify criminal activity, and suppress and reduce crime to improve safety for their citizens. Smart city technologies utilize a variety of Internet of Things (IoT) devices and sensors (both public and private) which are generally, but not always, limited to:

- Surveillance videos, home/business/public (some with facial recognition)
- License plate readers
- Enhanced public safety communications and 9-1-1 systems
- Deputies and police officers equipped with body-worn and vehicle-installed cameras
- Cellular telephones/towers
- Community-wide wireless Internet
- Social media communications
- Financial and credit card skimmers
- Advanced data systems tracking criminal activity and incident reports
- Drones
- Traffic control systems

Many sheriffs and police departments serving these communities now have state-of-the-art, 24 hour-a-day control centers monitoring activity using all these capabilities and providing “real- time” accuracy when crimes or other incidents occur. This allows them to respond and deploy law enforcement and other emergency assets more quickly than ever before.

These control centers are continually collecting high volumes of “big data” and information that are often beneficial when crimes occur — especially the violent crimes and homicides that plague many cities. The availability of this

data to those responsible for the investigations into these incidents has proven invaluable to developing leads, identifying suspects, gathering information, and even actionable intelligence — ultimately solving many of these crimes.

Cyber criminals have exploited the gaps inherent in the enforcement of Internet crimes and have created online marketplaces for transnational cyber criminals to share stolen information (credit card data, personally identifiable information (PII), and criminal methodologies). The progression of cybercrime from the early days of stolen payment card data to the development of the robust cybercriminal underground network it is today is responsible for offering cybercrime as a service — offering malware, exploit kits, and ransomware resulting in a billion-dollar market for fraud.

The types of cybercrimes and technology-facilitated financial crimes occurring today include:

- Child exploitation
- Human trafficking — adult and child sex trafficking
- Sale and distribution of illegal narcotics
- Acts of violence (murder, assault, rape)
- Fuel pump skimmers
- ATM skimmers
- ATM attacks
- Synthetic identity fraud
- Sextortion
- Illegal gun/weapon sales and distribution
- Third party money laundering
- Unlicensed MSBs
- Insurance and investment fraud
- BEC, romance scams, ransomware
- Digital currency theft
- Network intrusions
- Identity theft
- Bank/wire fraud
- Extortion
- Luring of children/abduction (sexual assault)
- Bullying, threats, intimidation, and others

The convergence of technology and the Internet, the ubiquitous nature of social media, diminished barriers to entry, and greater anonymity provided by the Internet allow criminals to conspire more easily and conduct their crimes on a local, state, national, and transnational basis. Complicating matters further is determining who has the authority to investigate and

prosecute these cases. It is not always clear or easy to define. The nature and wide scope of this activity have simply "blurred" or wiped away jurisdictional lines. Communities, states, and nations are no longer "self-contained" when it comes to cybercrime. Sadly, victims do not always know how and where to report.

> There's a technology component to every crime committed today.
>
> — Scott Cochran, Special Agent-in-Charge, Asset Forfeiture Division, U.S. Secret Service

In addition, police are faced with the daily challenges of providing community services and protecting life and property in the wake of ongoing reports of traditional "street crime" such as violence, illegal drug use/sales, burglaries robberies, homicides, and a host of other crimes. These demands forever continue while the need to "police" and protect victims in cyberspace increases at an overwhelming pace with already strained budgets.

The adverse financial and personal impact on people's lives continues to transform with every evolution of cyber scams and criminal activity. The Internet is an irretrievable component in society, an enabler of global commerce and growth. It is as much a force for good as it is a potential of risk to the very societal institutions and services, both civic and economic, upon which we have become dependent via a robust and safe Internet. It is estimated that one-half of the world's population utilizes the Internet and that, by the year 2030, there will be 125 billion IoT devices worldwide (2018 Ponemon Report on DNS Cybersecurity & Protection.) Today, the average person has in his/her possession, or immediately available, four Internet-connected devices (smartphones, tablets, computers, smart televisions, tracking or mapping devices, exercise bracelets, etc.).

What is the most serious threat out there? The short answer is there are many threats. Clearly criminals are using technologies to commit traditional crimes and, while these crimes are trending downward, the reality is that cybercrime is exploding. A report released recently by the FBI clearly shows the alarming rise in the number of crimes reported to the FBI's Internet Crime Complaint Center (IC3) (see below).

Most troubling is that the estimated number of fraud crimes reported to IC3 is merely an estimated 15 percent (The Changing Nature of Crime and Criminal Investigations PERF 2018 7). Many simply do not know where or how to report when they become victims. [2]

"The scale, scope, speed, and impact of cyber threats is constantly evolving," said FBI Cyber Division Assistant Director Matt Gorham. "Criminals are

opportunistic, and we've seen them rapidly adapt to the cyber environment, creating a variety of schemes to exploit the public and private sector" (see "The FBI's Internet Crime Complaint Center (IC3) Marks Its 20th Year," May 2020).

First, at an economic level, the biggest concern is criminal activity that could erode trust in our financial markets. There are criminal groups which incorporate increasingly sophisticated financial activity in their criminal schemes. Examples include obtaining unreleased business press releases to place financial trades or placing short positions and then engaging in damaging activity against the company. On a personal level, there has been an increase among criminals engaging in various cyber extortion schemes, from sextortion (capturing and threatening to release nude images or videos of a victim) to ransomware. These cyber extortion schemes have a very direct and personal impact on the victims.

Successful identification and mitigation of the ever-evolving nature of cyber threats is dependent on a myriad of factors, to include the development of adequate tools, risk assessments, incident response plans, and close partnerships between and among the private sector, academia, and the law enforcement community. A key component, however, in effectively countering this ubiquitous threat is the "People Problem." (Cybersecurity CEO: Top Conversations For The C-Suite In 2019 Robert Herjavec | Jan 14, 2019)

Today, cyber threats pose a significant threat to the nation's financial and payment systems and a growing risk to individual consumers or, otherwise, anyone who minimally interacts with online activity for financial, social, or other means. These threats are constantly evolving given the low barrier to entry and the risk-reward ratio for those who utilize the cyber realm for advancement of nefarious schemes. The public and private sectors, however, have taken great strides in the development of their capabilities and programs necessary to counter these threats.

Advances in computer technology and greater access to private corporate entities via the Internet have created online marketplaces for transnational cyber criminals to share stolen information (credit card data, personally identifiable information (PII), and criminal methodologies). Cyber criminals have become adept at stealing, trafficking, and fraudulently using sensitive information, to include PII data. They include organized criminal groups that operate transnationally and are multifaceted.

The reality is that this has become the unintended consequence of these advancements. Technology has unfortunately created opportunities for

criminals to migrate from traditional local street crimes to the world of cyberspace in committing their illegal activities — far less risk and "a safer place for them to operate." Cyber threats continue to grow in scale and sophistication at a remarkable pace. As an example, today there is an ever-growing presence of street gangs using computers, social media, and the Internet to commit their crimes. Sales of weapons and guns, illegal narcotics, financial crimes, theft, extortion, embezzlement, and adult and child sex trafficking are increasingly prevalent.

Gangs find cyberspace a much safer place where they can avoid the inherent dangers of committing street crimes and minimize the possibility of law enforcement detection and arrest.

When it comes to victims there is no demographic untouched — even our children are targets for victimization. Online sexual exploitation already has been at epidemic levels and continues to increase at alarming rates. Reports of sexual exploitation to the National Center for Missing and Exploited Children's Cyber-Tip Line have been skyrocketing over the past several years.

Driven by the popularity of online social media "app's" and online gaming devices, sexual offenders and predators are using these platforms to communicate directly with our children. This has moved sexual predators from public places such as parks, school bus stops, and street corners directly into our homes and children's bedrooms. There is increasing evidence of "sextortion" and online luring where, in some very disturbing cases, offenders have arranged to meet children for purposes of sexual victimization. In some very egregious cases offenders have lured children to their homes, violently sexually assaulted them, and held them captive for days and weeks.

While this threat has become an alarming reality, over the past several years we simultaneously experienced very noticeable and significant downward trends in the numbers of "stereotypical" child abductions (those where children were violently taken by offenders from parks, street corners, bus stops, and other public places). Ironically, these reductions are due to technology — AMBER Alerts, smart phone technology and social media, video cameras, etc., but these luring cases and sextortion arguably confirm that offenders are still motivated to victimize children. Many merely changed the way they go about it.

Although the law enforcement profession has made great strides in keeping up with the rapidity of technological advancement, due to financial, political, and jurisdictional constraints, all too often our police and sheriffs are illequipped or simply lack the authority outside their jurisdictions to combat

these crimes more effectively. More can be done to better leverage technology to help drive a more comprehensive, coordinated, and multifaceted investigative approach which relies on a whole-of-government concept through increased information sharing and collaboration. Partnerships are crucial because of information sharing, leveraging resources, and best practices. [3]

"Now, during the COVID 19 pandemic, scammers are working overtime hawking fake cures and investment schemes, selling protective equipment without the inventory on hand, and looking to take advantage of a more concentrated online presence during increased telework and distance learning arrangements ("The FBI's Internet Crime Complaint Center (IC3) Marks Its 20th Year," May 2020)."[4]

While not surprising there is even widespread fraud activity linked to COVID-19, including:

- Treatment scams: Scammers are offering to sell fake cures, vaccines, and advice on unproven treatments for COVID-19.
- Supply scams: Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.
- Provider scams: Scammers are also contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment.
- Charity scams: Scammers are soliciting donations for individuals, groups, and areas affected by COVID-19.
- Phishing scams: Scammers posing as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are sending phishing emails designed to trick recipients into downloading malware or providing personal identifying and financial information.
- App scams: Scammers are also creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and personal information.
- Investment scams: Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result. These promotions are often styled as "research reports," make predictions of a specific "target price," and relate to microcap stocks, or low-priced stocks issued by the smallest of companies with limited

publicly available information.
- Price-gouging scams: Individuals and businesses may sell essential goods, like hand sanitizer, for significantly higher prices than in a nonemergency setting. (Department of Justice, U.S. Attorney's Office, Eastern District of Virginia. See https://www.justice.gov/usao-edva/pr/federal-and-state-officials-launch-virginia-coronavirus-fraud-task-force.)

It is not just cybercrime; there are also technology components in nearly all other crimes. While there are significant challenges when it comes to responding to and investigating all these crimes, there are also great opportunities for law enforcement.

When it comes to the law enforcement response and investigations, technology is "both a blessing and a curse." Much like forensic and latent evidence at a crime scene, the opportunities lie within the "electronic trails and footprints" left behind that can often link the suspects directly to the crimes, their victims, or other suspects-providing conclusive or convincing circumstantial evidence, albeit requiring advanced analysis of overwhelming amounts of "big data."

The challenges are obvious, beginning with locating, identifying, and collecting electronic evidence data, the analysis of the data, and the associated costs of manpower, technology, and equipment. It has been estimated that today's police detective is spending between 32 and 36 hours per week reviewing and analyzing data on his/her cases! This leaves a mere 4-8 hours per week to work in the field (see Background on Cellebrite & Global Survey Insights–May 2019).[5]

For instance, for a typical homicide investigation the investigators often need to focus not only on the latent and forensic evidence collected at the scene, but also on the enormous amounts of data from the devices from at least three distinct sources — victim(s), witnesses, and suspects. By today's standards the amount of information derived from just the cellular or smart phones can "fill a room." This, of course, is if they are fortunate to have a likely suspect; otherwise, everyone identified or considered to be a suspect potentially may require extensive analysis of his/her devices and other technologies.[6]

Not just homicide[7] investigations yield this type and amount of data; nearly all investigations now do so. Hence, this is the problem — not many agencies are prepared to handle, evaluate, analyze, and make use of this amount of "big data," even though it often contains considerable evidence against suspects.

Cellular telephone and smartphones have long been “goldmines” of information for investigators — not only tracking the telephone activity, but also the instant messaging, social media activity, Internet use, video, photographs, and even GPS tracking capabilities in some cases. However, the criminals are keenly aware of this capability and have been practicing countermeasures to avoid detection — such as turning off devices or leaving them behind when committing crimes, relying on the use of “throw-away” or “burner” phones, or in some cases several of these devices, as just a couple of examples. There are also GPS and mapping devices on vehicles, Alexa devices, and smart televisions equipped with microphones and cameras in homes, and even social media that can sometimes be used to further investigations.

It is commonly known that a small number of individuals account for a large proportion of crime in a jurisdiction while recidivism rates of these offenders contribute to a cycle of crime impacting the quality of life of the public and placing undue restraints on the resources, people, and budgets of our police departments. The rapid rate of change in today’s global economy, which produces, distributes, and uses large amounts of data for public and private operations, presents newfound challenges to law enforcement’s ability to adapt and effectively respond to new threats.

RECOMMENDED ACTIONS

Continued Education and Training — Police organizations face an ever-evolving threat often enabled by the viability, low barriers to entry, and anonymity provided by the Internet and advances in technology. Successful mitigation of this risk necessitates a professionalized workforce that remains ahead of the advances made by organized criminal groups. Training is paramount to the success of all police professionals.

Some examples include:

United States Secret Service (USSS) National Computer Forensics Institute (NCFI, https://www.ncfi.usss.gov/ncfi/index.xhtml).

The National Computer Forensic Institute (NCFI) is a partnership among the U.S. Secret Service, the Department of Homeland Security, the state of Alabama, and the Alabama District Attorney’s Association to train state and local law enforcement, judges, and prosecutors in digital evidence, network intrusion, and computer/ mobile device forensic issues. NCFI training courses are offered complimentary for state, local, tribal, and territorial (SLTT) government attendees, through funding from the federal government. Run by

the U.S. Secret Service's Criminal Investigative Division and the Alabama Office of Prosecution Services, the training model is based upon the Secret Service's successful cyber investigative strategy, which relies on partnering with and sharing information among academia, private industry, and law enforcement/legal communities to combat the everevolving threat of cybercrime. The curriculum reflects current trends in the field and addresses potential technological obstacles as they are encountered in active investigations.

The International Association of Chiefs of Police (IACP), known to all police departments and law enforcement agencies for its commitment to issues pertinent to the police profession, is a vital resource for training and continued education. The IACP aids the law enforcement community in the form of publications, webinars, and training opportunities (https://www.theiacp.org/topics/education-training).

Additionally, the IACP Net, a professional service of the IACP, is another tool for assisting law enforcement officials to obtain necessary training and to exchange information and best practices in an effort to make informed, data-driven decisions (https://www.theiacp.org/IACPNet).

The National Sheriffs Association (NSA) is a professional law enforcement association dedicated to serving the Office of Sheriff and its affiliates through provision of education, training, and resources pertinent to policing and public safety (https://www.sheriffs.org/about-nsa/certifications-trainings).

Increased Utilization of Public/Private Sector Partnerships and Technology

Even the largest agencies are not fully equipped, sufficiently resourced, or have the adequate number of personnel to handle, respond, investigate, curb, and eradicate cybercrime and/or investigate traditional crimes with technological components. Law enforcement leaders need to consider abandoning long-standing paradigms of self-containment and consider expanding public/private partnerships to help them resolve the overwhelming problem of effectively and adequately managing "big data."

The next generation policing platform, the Accurint® Virtual Crime Center (AVCC), is currently helping police succeed in a proactive-based approach to combat rising crime trends. It provides a comprehensive solution to law enforcement agencies that a place to link crossjurisdictional data with public records in one interface to help them predict and solve crime. The AVCC tool

allows for the secure access to law enforcement data from neighboring agencies and from agencies across the country to build a complete picture of individuals, locations, and incidents. This cutting-edge investigative technology can expedite the identification of people and their assets, addresses, relatives, and business associates by providing instant access to a comprehensive database of public records that would ordinarily take days to collect. AVCC is a next-generation policing platform used for COMPSTAT, Analytics, Crime Analysis, and Investigations. This solution links billions of public records to agency-provided data in a cross-jurisdictional data exchange to provide law enforcement with unprecedented visibility into crime in its own jurisdiction and around the country. Linking across data types delivers a more comprehensive view into an identity, helping law enforcement to target investigations, identify patterns, and deploy resources more efficiently.

Resolving these issues lies within the opportunities. A high number of cases may be solved leveraging today's technology. Investigators must be able to identify the sources and what is available, knowing how to retrieve and preserve the data legally, and then what to do with the tremendous amount of "big data" sent back to them. Managing the amount of information available can be overwhelming and become "sensory overload." Within that data is often conclusive evidence or even strong circumstantial information helpful to their investigations that must be analyzed and linked into an understandable and coherent format which may be used to convict those responsible. This certainly cannot be adequately performed manually and requires advanced analytics capabilities.

In October 2019, LexisNexis® Risk Solutions released its Cybercrime Report providing a comprehensive view into the shifting global fraud landscape from January 2019 through June 2019. The report leverages the LexisNexis® Digital Identity Network, which is a system built on crossindustry identity intelligence and analyzes millions of transactions daily in real time across billions of devices for thousands of global digital businesses. For the sixmonth time frame of the report, the LexisNexis Digital Identity Network recorded 16.4 billion transactions, of which 277 million were human-initiated attacks, a 13 percent increase over the second half of 2018.

The report highlights a shift toward networked, crossorganizational, and cross-industry fraud, and gives insight into the evolution of bot attacks targeting new accounts in media and e-commerce. "Although this report focused on the private sector, the LexisNexis Risk Solutions Cybercrime Report is a must read for federal IT managers and law enforcement agencies," suggested Haywood Talcove, CEO for Government. "Agencies need to use a layered approach to cybersecurity if they want to remain protected," insisted

Talcove. “A better solution includes three components: high-level digital identity intelligence, physical identity, and authentication capabilities. These three components will help agencies meet regulatory requirements, improve user experience, and locate evolving fraud. If this approach is executable in near real time, it allows for more streamlined regulatory compliance processes and reduces friction across the citizen experience.”[8]

Among the concerns for police and government agencies is the ability to leverage data, analytics, and insights to help protect against increasingly complex and ubiquitous fraud scams. The proliferation of transnational financial fraud schemes and cybercrime has contributed to the increased number of new businesses and vendors created to gain access to the new COVID-19 stimulus funding. This type of financial and cyber-enabled fraud is but one example by which technological tools would help mitigate and instill up-front fraud prevention measures to assess risk and streamline business and vendor due diligence.

Law enforcement agencies need instant access to comprehensive public records data and advanced analytics to generate quality investigative leads, produce actionable intelligence, and drive informed decisions. Law enforcement can no longer afford to minimize or avoid the costs of new technologies and analytics skill sets. Detectives need to be on the street doing what they do best — not tethered to a computer terminal analyzing data that should be readily available to them.

The challenge for today’s investigators lies within the opportunities. A high number of cases may be solved leveraging today’s technology. Investigators must be able to identify the sources and what is available, knowing how to retrieve and preserve the data legally, and then what to do with the tremendous amount of “big data” sent back to them. Managing the amount of information available can be overwhelming and become “sensory overload.” Within that data is often conclusive evidence or even strong circumstantial information helpful to their investigations that must be analyzed and linked into an understandable and coherent format that may be used to convict those responsible. This certainly cannot be adequately performed manually and requires advanced analytics capabilities.

This advancement is only made possible by the sharing of vital information across city and state boundaries which enables investigators more easily to identify and understand the nature, patterns, and trends of the offenders while tracking and evaluating the evolution of their criminal involvement using our new data-driven policing tools. The need for better use of technology, combined with a strategic approach to policing and use of available private sector solutions to these complex problems, is safeguarding

the interests and liberties of our communities and its people.

A multiagency and multifaceted investigative approach is required to address the cross-jurisdictional nature of crime adequately. The transnational element of crime enabled by the widespread use and ease of access to computers calls for subject matter experts with the analytical mindset and capabilities to support criminal investigations. One example of a successful model is the Special Investigations Unit (SIU) of LexisNexis. The SIU is comprised of former law enforcement experts who leverage the LexisNexis solutions and data offering to provide real-time investigative insight.

SIU helps law enforcement analyze data, find patterns, and leverage the full suite of LexisNexis' offerings to solve, manage, and predict crime. SIU analysts with extensive experience in investigations, patrol activities, intelligence analysis, and crime analysis focus exclusively on law enforcement. The SIU can leverage detailed law enforcement data contributed from agencies across the country including detailed RMS, CAD, Field Contact, Accidents, and Offender data and combine this with extensive public records data as well as social media analytics. LexisNexis Risk Solutions is a long-time, trusted, and proven law enforcement partner which has the best-trained analysts equipped with the latest technologies. The LexisNexis Special Investigations Unit is staffed with some of the very best in our nation today. The SIU model is a proven way to help leverage the power of the private sector in support of specific law enforcement and homeland security missions. The SIU embeds itself and works alongside those public servants who are entrusted to fight fraud and keep our communities safe.

1. Breslin, Michael. "Robbery Without Borders." Security Management Magazine, August 2019.

2. NEW NATIONAL COMMITMENT REQUIRED: The Changing Nature of Crime and Criminal Investigations. Police Executive Research Forum (PERF), January 2018. https://www.policeforum.org/assets/ChangingNatureofCrime.pdf.

3. Breslin, Michael. "Collaboration between Resourcing and Operations: Keys to Mission Success." The Journal of Government Financial Management, Vol. 67, no. 1 (April 2018).

4. "The FBI's Internet Crime Complaint Center (IC3) Marks Its 20th Year." FBI. May 8, 2020. https://www.fbi.gov/news/pressrel/press-releases/the-fbis-internet-crime-complaint-center-ic3-marks-its-20th-year.

5. Cellebrite. “Background on Cellebrite & Global Survey Insights,” May 2019.

6. Matthews, Kayla. “How Data Analytics Are Solving Murders.” Towards Data Science, July 23, 2019. https://medium.com/data-science/how-data-analytics-are-solving-murders-1cdac5432d6e.

7. LexisNexis® Risk Solutions. Rep. FRAUD WITHOUT BORDERS: An Analysis of Global Cybercrime Across Industries and Geographies, 2019.

8. : New 2019 Cybercrime Report Tracks Growing Threat of Networked Cybercrime https://risk.lexisnexis.com/about-us/press-room/press-release/20191022-gov-cybercrime

WHAT THE FUTURE HOLDS

In a post-9/11 world, information sharing among law enforcement and homeland security professionals, although improved, requires more to be done. Information sharing is still a problem and poses a gap which criminal groups are more than capable of exploiting. The intelligent and purposeful use of big data will help fill this void. The increased complexity and networked attributes of criminal activity which often take on a transnational significance require a cross-functional response by law enforcement.

The actionable commitment to information sharing requires more than a willingness to collaborate; it requires the further establishment of cooperation agreements, the proper technology, and tools to share information across jurisdictional boundaries. Police need better data analytics to enable the increased use of actionable intelligence — to help solve crimes, identify, arrest, and dismantle criminal networks. A strategic plan is necessary to identify and purchase the appropriate analytical tools as well as increased spending to ensure the most current technology is used.

Emerging technology represents a powerful new tool for criminals due, in part, to the diffused decision-making systems, ease by which to avoid detection, and foreignbased influence. The police face formidable threats. These threats are plentiful and often decentralized in nature as in the case of transnational criminal organizations, nation state actors, sophisticated cyber criminals, and terrorists. Many criminal activities of the past are no longer just local crimes.

The lines between the origin and end point of criminal activity are often blurred and difficult to apply attribution due to advances in technology, use of the Internet, and foreign networks. Crime has moved into the digital world. Criminals and the police charged with catching them all work in a hyper-competitive environment. Both groups compete for limited resources to fulfill their objectives. The end state for criminals is money, influence, and power, whereas for law enforcement it is the ability to gain the necessary advantage to combat and eradicate criminal activity and safeguard the public. More must be done to provide law enforcement the proper tools to accomplish this noble goal.

The scope and sophistication of technology-related crimes and cybercrime are continually expanding and changing. The existence of the “dark web” and encryption are both creating opportunities for criminals to remain completely anonymous. Law enforcement faces huge obstacles in combating crime in this modern-day equivalent of the “Wild West.” Many technology companies have already encrypted their data or are moving rapidly toward encryption to protect the privacy of users. While on its surface this appears to be a very noble gesture that is embraced by privacy rights advocates and groups, the implications are frightening. There is no easy solution to these issues.

While this situation is troubling, law enforcement today remains well-positioned when it comes to using technology to promote community safety, prevent crime, and investigate it. Much of the data is readily available from community-owned devices, while others come from a variety of private sources, such as businesses, homeowners, and private providers or companies. Investigators must remain current on what sources are available, the requirements and procedures for securing the data, how to preserve the information during the process, and the capabilities or potential use.

Identifying and obtaining the data is only part of the solution; the dilemma lies in what to do with the overwhelming mountain of information or “big data.” To make best use of the information, law enforcement agencies need trained analysts equipped with the latest analytic technologies. In today’s environment this is no longer a luxury; it is a necessity. Detectives in many agencies are spending far too much valuable time tethered to computers and other devices trying to locate bits and nuggets of information necessary to help them solve their cases. This is time that may be better served on the street protecting communities and investigating cases.

This represents a significant paradigm shift for law enforcement where many have embraced technology as part of their mission while some face difficulties in keeping up and adapting to this changing world. The solutions should focus on the following areas:

1. Agency commitment to embracing and utilizing technology to protect the community and investigate crimes.
2. Recruitment of new officers and analysts with the appropriate skills.
3. Agency-wide advanced training to identify the available capabilities and sources of data.
4. Securing up-to-date and enhanced analytical systems to manage and interpret “big data.”

Of course, because all of this comes at a cost, law enforcement leaders must consider creative and innovative ways to manage and keep costs down, like

pooling resources with other agencies (a multijurisdictional approach and cost-sharing model), public/ private partnerships, or simply outsourcing analytical responsibilities to private law enforcement contractors. Many solutions are readily available.

About Authors

Michael Breslin is a Law Enforcement and Homeland Security Professional. He is a retired federal law enforcement senior executive with 24 years of law enforcement and homeland security experience. His career was spent with the U.S. Secret Service, serving as Deputy Assistant Director in the Office of Investigations with oversight of 162 domestic and foreign field offices. He earned a BA degree from Saint John's University in Queens, NY. He also holds an MS in National Security Strategy and a graduate certificate in Business Transformation and Decision Making from the Industrial College of the Armed Forces [now the Eisenhower School of National Defense University] and an MPA from the John Jay College of Criminal Justice. Currently he serves on the Board of Directors for the National Center for Missing and Exploited Children (NCMEC). Michael has also published numerous articles on homeland security, defense, and threat mitigation methods.

Robert G. Lowery, Jr., is retired Vice President, Missing Children Division, NCMEC. He currently provides training forlaw enforcement on behalf of the U.S. Department of Justice. He has over 30 years of law enforcement experience having served as Assistant Chief of Police for the Florissant, Missouri, Police Department and was Commander of the Greater St. Louis Major Case Squad. He was directly responsible for homicide and violent crime investigations in the entire St. Louis metropolitan region. He is the author of several law enforcement publications on the topics of investigation of violent crime, homicide, unidentified human remains, abducted and missing children, and missing children with special needs. Bob holds a BA degree (summa cum laude) and an MS in Human Resource Management from Lindenwood University. He is also a graduate of the FBI National Academy at Quantico.